

1 JOHN P. FLYNN (State Bar No. 141094)
jflynn@wsgr.com
2 STEFANI E. SHANBERG (State Bar No. 206717)
sshanberg@wsgr.com
3 JENNIFER J. SCHMIDT (State Bar No. 295579)
jschmidt@wsgr.com
4 ROBIN L. BREWER (State Bar No. 253686)
rbrewer@wsgr.com
5 EUGENE MARDER (State Bar No. 275762)
emarder@wsgr.com
6 MADELEINE E. GREENE (State Bar No. 263120)
mgreene@wsgr.com
7 MICHAEL J. GUO (State Bar No. 284917)
mguo@wsgr.com
8 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
9 One Market Plaza
Spear Tower, Suite 3300
10 San Francisco, California 94105
Telephone: (415) 947-2000
11 Facsimile: (415) 947-2099

12 Counsel for Defendant
BLUE COAT SYSTEMS LLC
13
14

15 IN THE UNITED STATES DISTRICT COURT
16 FOR THE NORTHERN DISTRICT OF CALIFORNIA
17 SAN JOSE DIVISION

18 FINJAN, INC., a Delaware Corporation,

19 Plaintiff,

20 v.

21 BLUE COAT SYSTEMS LLC, a Delaware
Corporation,

22 Defendant.
23

CASE NO.: 15-cv-03295-BLF-SVK

**DEFENDANT BLUE COAT SYSTEMS
LLC'S MOTION FOR SUMMARY
JUDGMENT OF NONINFRINGEMENT**

Date: June 22, 2017

Time: 9:00 a.m.

Place: Courtroom 3, 5th Floor

Judge: Honorable Beth Labson Freeman

24 **REDACTED VERSION OF DOCUMENT**
25 **SOUGHT TO BE SEALED**
26
27
28

TABLE OF CONTENTS

	Page
TABLE OF CONTENTS	i
TABLE OF AUTHORITIES	iii
TABLE OF ABBREVIATIONS	iv
NOTICE OF MOTION AND MOTION	v
MEMORANDUM OF POINTS AND AUTHORITIES	1
I. INTRODUCTION	1
II. BACKGROUND	2
A. Finjan’s Allegations	2
B. Accused Products Relevant to Motion for Summary Judgment	3
III. LEGAL STANDARD	5
IV. Blue Coat Does Not Infringe Claim 1 of the ’580 Patent (“The SSL Patent”).	5
A. SSLV and ProxySG cannot “communicate[] to” each other	8
B. ProxySG and SSLV cannot communicate a “reply message” or “cached attributes of the signed server certificate” to each other and do not have a “certificate comparator.”	9
C. SSLV and ProxySG do not share the claimed “non-SSL connection.”	11
D. SSLV does not perform an “SSL handshake with the client computer.”	13
V. Blue Coat Does Not Infringe Claim 22 of the ’408 Patent (“The Parse Tree Patent”).	14
A. DRTR does not “determin[e] any specific one of a plurality of programming languages.”	15
B. DRTR does not “instantiate[e] a scanner . . . in response.”	17
C. DRTR does not analyze an “incoming stream” of program code.	17
VI. Blue Coat Does Not Infringe Claim 1 of the ’786 Patent.	18
A. No “sandboxed package including the mobile protection code . . . [is] communicated.”	20

1	B. MAA is not an “information-destination.”	21
2	C. Blue Coat products do not infringe the '786 patent under the	
3	doctrine of equivalents.....	22
4	VII. Blue Coat’s “WebPulse/GIN” Product Does Not Perform Sandboxing.	23
5	VIII. CONCLUSION	25

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

Page(s)

CASES

Anderson v. Liberty Lobby, Inc., 477 U.S. 242 (1986) *passim*

Asyst Technologies, Inc. v. Emtrak, Inc., 402 F.3d 1188 (Fed. Cir. 2005)22

Becton Dickinson & Co. v. C.R. Bard, Inc., 922 F.2d 792 (Fed. Cir. 1990).....5

Celotex Corp. v. Catrett, 477 U.S. 317 (1986).....5

Finjan Inc. v. Blue Coat Sys., Inc., No. 13-03999 BLF, 2014 WL 5361976 (N.D. Cal. Oct. 20, 2014)18, 19, 20

Litton Sys. Inc. v. Honeywell, Inc., 140 F.3d 1449 (Fed. Cir. 1998)5, 14, 18, 23

Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp., 475 U.S. 574 (1986).....5

Rotec Indus., Inc. v. Mitsubishi Corp., 215 F.3d 1246 (Fed.Cir.2000)25

Technology Licensing Corp. v. Videotek, Inc., 545 F.3d 1316 (Fed. Cir. 2008).....5

Wavetronix LLC v. EIS Electronic Integrated Systems, 573 F.3d 1343 (Fed. Cir. 2009).....22, 23

STATUTES

35 U.S.C. § 1125, 6

35 U.S.C. § 271(a).....25

RULES

Fed. R. Civ. P. 565, 15

TABLE OF ABBREVIATIONS

Plaintiff Finjan, Inc.	Finjan or Plaintiff
Defendant Blue Coat Systems LLC	Blue Coat or Defendant
Deposition Transcript of Dr. Eric Cole	Cole Dep. Tr.
Deposition Transcript of Dr. Michael Mitzenmacher	Mitzenmacher Dep. Tr.
Deposition Transcript of David Wells	Wells Dep. Tr.
Deposition Transcript of Christian Larsen	C. Larsen Dep. Tr.
Deposition Transcript of Christophe Birkeland	Birkeland Dep. Tr.
Deposition Transcript of Kevin Rohan	Rohan Dep. Tr.
Expert Report of Michael Mitzenmacher	Mitzenmacher Rpt.
Expert Report of Eric Cole	Cole Rpt.
Expert Report of Nenad Medvidovic	Medvidovic Rpt.
U.S. Patent No. 6,154,844	'844 patent
U.S. Patent No. 6,965,968	'968 patent
U.S. Patent No. 7,418,731	'731 patent
U.S. Patent No. 8,079,086	'086 patent
U.S. Patent No. 8,225,408	'408 patent
U.S. Patent No. 8,566,580	'580 patent
U.S. Patent No. 8,677,494	'494 patent
U.S. Patent No. 9,141,786	'786 patent
U.S. Patent No. 9,189,621	'621 patent
U.S. Patent No. 9,219,755	'755 patent
'844, '968, '731, '086, '408, '580, '494, '786, '621, and '755 patents, collectively	asserted patents
SSL Visibility Appliance	SSLV
Malware Analysis Appliance	MAA
Dynamic Real Time Rating	DRTR
Global Intelligence Network	GIN
Content Analysis System	CAS
Advanced Secure Gateway	ASG
Web Security Service	WSS
Malware Analysis Service	MAS

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD HEREIN:

PLEASE TAKE NOTICE that on June 22, 2017, at 9:00 a.m., or as soon thereafter as the matter may be heard, in the courtroom of the Honorable Beth Labson Freeman, located at Courtroom 3, Fifth Floor of the United States District Court for the Northern District of California, San Jose Division, Defendant will and hereby does move this Court for an order granting summary judgment of no infringement as to U.S. Patent Nos. 8,566,580; 8,225,408; and 9,141,786, and all allegations as to “WebPulse/GIN sandboxing.”

This motion is made pursuant to Federal Rule of Civil Procedure 56. This motion is based on this notice of motion and motion, the supporting memorandum of points and authorities, the accompanying declarations, filed concurrently herewith, including exhibits, and such additional evidence and arguments as may hereinafter be presented.

MEMORANDUM OF POINTS AND AUTHORITIES**I. INTRODUCTION**

Finjan has done nothing to narrow this case. By dropping only redundant asserted claims, Finjan has reduced the number of claims without eliminating any patents or infringement theories. In fact, Finjan currently maintains scores of infringement theories, all of which are flawed and many of which are nonsensical. Thus, while the majority of Finjan's theories are amenable to summary judgment, Blue Coat has selected for this motion the four issues of noninfringement that will most narrow this case, i.e., by completely eliminating three patents, one product, and one alleged product combination, thereby making it more understandable for a jury.

Blue Coat seeks summary judgment on the '580 patent relating to SSL decryption and transmission. Blue Coat's product architecture is fundamentally different than the claimed architecture. The '580 claims require two SSL connections and one non-SSL connection. Blue Coat's products—like the prior art Finjan overcame to obtain the '580 patent—do not allow for any non-SSL connection. Next, Blue Coat seeks summary judgment on the '408 patent relating to building a parse tree. The '408 claims require identifying a programming language, applying rules specific to that programming language, and building a parse tree in real-time, none of which the Blue Coat products do. Blue Coat also moves for summary judgment on the '786 patent, which requires wrapping an executable file in mobile protection code and sending it to an end user computer so that it is safer to execute on that computer. In sharp contrast, Blue Coat's system executes files on an intermediary computer that need not be protected at all, representing a fundamentally different concept and architecture. Finally, Blue Coat moves for summary judgment on all allegations related to nonexistent product functionality that Finjan imagined: "WebPulse/GIN sandboxing." WebPulse/GIN sandboxing does not exist, and Finjan's attempt to ensnare more Blue Coat products for its damages case should be rejected.

The evidence Finjan purports to rely upon is thin and strained—where it exists at all. No reasonable jury could find in Finjan's favor on these theories. Rather than triable issues of fact, Finjan relies on obfuscation and confusion. Blue Coat respectfully requests that this Court find noninfringement on each of these theories as a matter of law.

II. BACKGROUND

A. Finjan's Allegations

On August 28, 2013, Finjan filed a Complaint against Blue Coat, asserting infringement of six patents. *Finjan, Inc. v. Blue Coat Systems LLC*, Case No. 13-cv-03999-BLF (N.D. Cal. Aug. 28, 2013), Dkt. No. 1. Finjan's allegations concerned a number of Blue Coat products, including ProxySG, WebPulse, CAS, and MAA. *Finjan, Inc. v. Blue Coat Systems LLC*, Case No. 13-cv-03999-BLF (N.D. Cal. July 13, 2015), Dkt. No. 374 at 1. While that litigation was still pending, Finjan filed a second complaint against Blue Coat on July 15, 2015, asserting infringement of 10 patents, three of which overlap with those at issue in the first suit. *See* Complaint, Dkt. No. 1. Finjan's allegations are directed to a broad range of Blue Coat products, including the ProxySG, WebPulse, CAS, and MAA products accused in the first suit. *Id.* at 6. Finjan filed its final election of asserted claims on February 27, 2017 and served infringement expert reports on March 29, 2017. Exh. 1¹ (Plaintiff Finjan Inc.'s Final Election of Asserted Claims (Feb. 27, 2017)); Exh. 2 (Mitzenmacher Rpt.); Exh. 3 (Cole Rpt.); Exh. 4 (Medvidovic Rpt.). The following chart summarizes Finjan's allegations, as articulated in its infringement expert reports:²

Patent	Asserted Claims	Accused Products
'844	1, 7, 15	WebPulse/GIN; WSS with WebPulse/GIN; WSS with MAS; ASG with MAA, SA with MAA
'731	1, 2	ASG with MAA; WSS with WebPulse/GIN; WSS with MAS
'968	1	ASG with MAA; WSS with WebPulse/GIN; WSS with MAS
'086	24	WebPulse/GIN; WSS with WebPulse/GIN; WSS with MAS, SA with MAA
'494	10, 14, 16	WebPulse/GIN; WSS with WebPulse/GIN; WSS with MAS; ASG with MAA; ProxySG and CAS with MAA; SA with MAA
'621	1, 10	WebPulse/GIN; WSS with MAS; ProxySG and CAS with MAA; ASG with MAA
'755	3	ProxySG and CAS with MAA; ASG with MAA

¹ All exhibits refer to the Declaration of Eugene Marder in Support of Blue Coat's Motion for Summary Judgment, filed concurrently herewith.

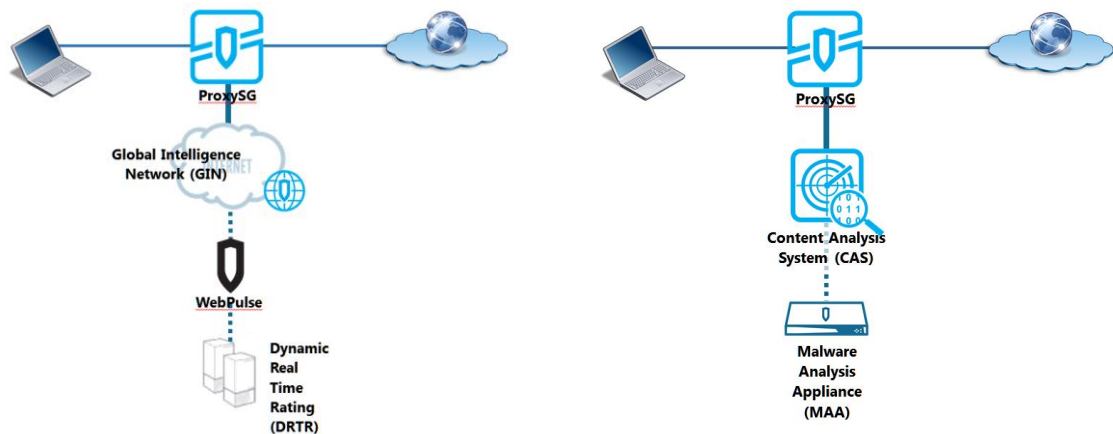
² As set forth in its Motion to Strike, Blue Coat believes that certain infringement theories and product combinations were not identified in Finjan's Infringement Contentions, and therefore cannot be asserted in this litigation. *See* Defendant Blue Coat Systems LLC's Motion to Strike Portions of Expert Reports, Dkt. No. 203. Nevertheless, the chart above sets forth a complete list of Finjan's allegations, as they appear in Finjan's infringement expert reports.

'786	1	WebPulse/GIN; WSS with MAS; ProxySG and CAS with MAA; ASG with MAA
'580	1	SSLVA with ProxySG
'408	22	WebPulse; WSS with WebPulse

B. Accused Products Relevant to Motion for Summary Judgment

The Blue Coat products at issue in this litigation are deployed at a network gateway—either through physical network appliances or cloud-based services—and include a variety of network optimization and security solutions, including threat analysis, web filtering and categorization, sandboxing, forensic analysis of threats, and inspection of secure traffic. Although Finjan accuses a number of overlapping products and combinations across each of the asserted patents, the bulk of the accused functionality comes from just a few accused products: the standalone SSLV appliance (relevant to the '580 patent), the DRTR component of WebPulse/GIN (relevant to the '408 patent), and MAA (relevant to the '786 patent).

SSLV is a dedicated appliance for Secure Sockets Layer (“SSL”) inspection, decryption, and management. Exh. 5 (BC2-0024375). When used for in-line SSL inspection, SSLV acts as a transparent proxy. *Id.* SSLV is then able to decrypt and inspect SSL-encrypted content, which would otherwise be obscured. Exh. 6 (BC2-0003898-901). In certain deployments, SSLV may be used in-line with a ProxySG. Exh. 7 (BC2-0024424-428). SSLV is frequently used in stand-alone deployment but is accused of infringing the '580 patent only in combination with ProxySG.



DRTR and **MAA** are the accused content scanning components in the Blue Coat ecosystem. Both DRTR and MAA are employed in scanning content by a network gateway—the ProxySG—as shown in the figures above. Specifically, **ProxySG** acts as a gateway between the

1 network and the internet. *See, e.g.*, Exh. 14 (BC2-0038344); Exh. 15 (BC2-0005494-496). When
 2 further analysis of unknown URLs is needed, ProxySG queries the WebPulse service, which
 3 includes the DRTR component. For further analysis of unknown files received in response to a
 4 content request, ProxySG queries an attached CAS, if available, which can in turn send content to
 5 MAA, if available, for inspection. *See, e.g.*, Exh. 12 (BC2-0020764-774); Exh. 16 (Sorgic Dep.
 6 Tr.) at 153:8-13.

7 DRTR performs analyses on a requested URL and attempts to determine applicable
 8 content categories and a risk level. Exh. 11 (C. Larsen Dep. Tr.) at 116:24-25, 143:3-8. DRTR
 9 ultimately provides ratings for URLs that have not already been categorized and is a component of
 10 the WebPulse service. **WebPulse** provides categorization and a risk level for URLs. *Id.* at 143:3-
 11 8. For example, if a requested URL is not located in its local database, ProxySG will send the
 12 URL to WebPulse for analysis. *See, e.g.*, Exh. 12 (BC2-0020764). WebPulse, in turn, is a service
 13 within GIN. **GIN** is the umbrella name given to Blue Coat's suite of connected intelligence
 14 services. Exh. 13 (Runald Dep. Tr.) at 11:14-16. "WebPulse/GIN,"³ alone and with WSS, is
 15 accused of infringing the '786 and '408 patents.

16 **MAA** is a file inspection appliance for performing dynamic analysis, or "sandboxing,"
 17 meaning detonation and observation of an unknown file to determine its risk level. *See* Exh. 8
 18 (BC2-0003245-248). MAA uses a combination of static and dynamic analysis techniques to
 19 identify malware. *Id.* By emulating or virtualizing a typical client environment, MAA can detect
 20 any harmful behavior in the file and determine whether it is a threat before it ever reaches a client.
 21 *Id.* MAA can then inform CAS of the file's risk score, enabling CAS to undertake further
 22 processing. *See generally* Exh. 9 (BC2_SC_001578-581); Exh. 10 (BC2_SC_000577-590).
 23 MAA allegedly provides the necessary and primary accused functionality in the product
 24 combinations accused of infringing the '786 patent.

25 For context, **CAS** is a content inspection appliance that ProxySG can utilize for additional
 26 analysis of files. Exh. 17 (BC2-0038296-298). If CAS cannot identify an object as either known

27 ³ While Blue Coat adopts Finjan's nomenclature herein, Finjan's use of the misnomer
 28 "WebPulse/GIN" improperly conflates WebPulse and GIN, which are distinct products.

1 good or known bad, the object can be sent to MAA for sandboxing. *See, e.g.*, Exh. 18 (T. Larsen
 2 Dep. Tr.) at 33:9-15. **ASG** is a product that combines the functionality of ProxySG and CAS in a
 3 single appliance. *See, e.g.*, Exh. 16 (Sorgic Dep. Tr.) at 13:2-4. Similarly, **WSS** is a product that
 4 combines much of the functionality of ProxySG and CAS in a web-hosted service. *See, e.g.*, Exh.
 5 19 (Maxted Dep. Tr.) at 14:13-16. **MAS** is Blue Coat’s term for certain MAA functionality
 6 available as a cloud-implemented service that can be used in conjunction with WSS. *See*
 7 *generally* Exh. 20 (FINJAN-BLCT 493638-640).

8 **III. LEGAL STANDARD**

9 Summary judgment may be granted where there exists no genuine dispute of material fact
 10 and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56. “[T]he mere
 11 existence of some alleged factual dispute between the parties will not defeat an otherwise properly
 12 supported motion for summary judgment; the requirement is that there be no genuine issue of
 13 material fact.” *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986). In order to defeat
 14 summary judgment, the non-moving party must set forth “specific facts showing that there is a
 15 genuine issue for trial.” Fed. R. Civ. P. 56(e); *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio*
 16 *Corp.*, 475 U.S. 574, 587 (1986). Moreover, where the nonmoving party will bear the burden of
 17 proof at trial—such as here—the moving party can prevail merely by pointing out to the district
 18 court that there is an absence of evidence to support the nonmoving party’s case. *Celotex Corp. v.*
 19 *Catrett*, 477 U.S. 317, 323 (1986).

20 Patent cases are appropriate for summary judgment. *See Becton Dickinson & Co. v. C.R.*
 21 *Bard, Inc.*, 922 F.2d 792, 795 (Fed. Cir. 1990). The patentee bears the burden of proving
 22 infringement. *See Technology Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1327 (Fed. Cir.
 23 2008). A claim is infringed only if every limitation is found in the accused product or process,
 24 and any deviation from the claim precludes a finding of infringement. *Litton Sys. Inc. v.*
 25 *Honeywell, Inc.*, 140 F.3d 1449, 1454 (Fed. Cir. 1998). If an independent claim is not infringed,
 26 each of the corresponding dependent claims cannot be infringed. *Becton Dickinson*, 922 F.2d at
 27 798; 35 U.S.C. § 112 ¶ 4.

28 **IV. Blue Coat Does Not Infringe Claim 1 of the ’580 Patent (“The SSL Patent”).**

The network architecture described and claimed by the '580 patent provides an efficient way to transfer encrypted content within a network, a system vastly different from the architecture of the accused Blue Coat products. As shown in Figure 2 above, the architecture of the '580 patented system requires that two security gateway computers coordinate to “split” an encrypted Secure Socket Layer (“SSL”) connection between a requesting client and content server—the first security gateway computer is connected to the client and the second security gateway computer is

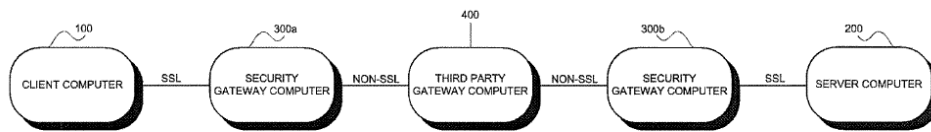


FIG. 2

connected to the server. See '580 patent at 3:24-31. In “splitting” the SSL

encrypted connection, these two security gateway computers share the key feature of the '580 patent: a non-SSL connection that allows the two security gateway computers to freely transmit unencrypted content between one-another and to other intermediary security devices, thereby avoiding the burden of establishing additional SSL connections between the security computers and any intermediaries. See *id.* at 4:1-5.

The system of claim 1 requires that the client computer and the first security computer share an encrypted SSL connection; the first security computer and the second security computer share a non-SSL connection; and the second security computer and the server computer share an encrypted SSL connection. See, e.g., *id.* at Fig. 2. After the client computer makes a request for SSL-encrypted content from a content server, the first security computer sends a connection request including cached certificate attributes for the server, if it already has any, to the second security computer. *Id.* at 5:22-6:42. The second security computer receives a certificate from and performs a handshake with the content server, then replies to the first security computer with certificate attributes of the current certificate, if the attributes in the connection request were outdated or missing. *Id.* The first security computer updates its proxy certificate, if necessary, and handshakes with the client. *Id.*

Unable to identify a system that operates according to the claimed architecture of the '580 patent, Finjan accuses two independent Blue Coat devices—SSLV and ProxySG—of infringing

claim 1 of the '580 patent. *See* Exh. 3 (Cole Rpt.) at ¶ 24. While each of these devices has the ability to inspect SSL communications individually, neither of them operates cooperatively to do so. *See* Exh. 7 (BC2-0024427) (“In this architecture SSL traffic is decrypted twice, once on the ProxySG and then again on the SSL Visibility Appliance.”). Rather, each must decrypt, inspect, and re-encrypt the SSL content, even when both are deployed in the accused arrangement. *See* Exh. 21 (Cole Dep. Tr.) at 77:15-21 (“Q. This connection that it’s referring to between the [ProxySG and SSLV] is an

SSL connection, correct?

A. It’s not labeled . . . but it

could potentially be that

SSL connection they’re

referring to.”). Accordingly, the structure of the accused Blue Coat system is precisely what Finjan sought to supersede with its patented invention. Exh. 22 (Medvidovic Dep. Tr.) at 327:12-15 (“[T]he point is that between the two security gateway computers, the connection is non-SSL as opposed to prior work which has these SSL connections throughout.”). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Another key distinction between the '580 patent and the accused Blue Coat products is that SSLV and ProxySG each act as “transparent” proxies. *See* Exh. 23 (BC2-1607593) (“When used in Active-Inline (AI) mode or Passive-Inline (PI) mode the SSL Visibility Appliance acts as a fully transparent proxy: the Ethernet ports used to connect it to the data network do not have IP addresses, and the other devices in the network are unaware that the SSL Visibility Appliance has been installed.”). This means that, even in Finjan’s alleged “infringement scenario,” [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Thus, they do not and

cannot work in conjunction with one another to “split” the SSL connection in the manner

1 prescribed by the asserted claim. '580 patent at 3:24-27; [REDACTED]

2 [REDACTED]
 3 [REDACTED] This "transparent" functionality
 4 allows SSLV to, for example, [REDACTED]

5 [REDACTED]
 6 Comparing the elements required by asserted claim 1 of the '580 patent to the accused
 7 Blue Coat products illustrates how strained Finjan's infringement theory is. Finjan's infringement
 8 allegations are often ambiguous and contradictory. For example, while claim 1 requires two
 9 security computers, each of which has distinct functions, Finjan's allegations frequently switch the
 10 roles between the accused ProxySG and SSLV products, conflate the required functionality, and
 11 fail to articulate a consistent infringement theory. Because Dr. Cole confirmed that in the alleged
 12 "infringement scenario," SSLV is the first security computer and ProxySG is the second security
 13 computer, that is the manner in which the accused product combination is addressed here. *See*
 14 Exh. 21 (Cole Dep. Tr.) at 35:21-36:3. The fatal flaws in Finjan's infringement theory thus
 15 underscore the utter absence of a genuine issue of material fact as to the requirements of the '580
 16 patent and the operation of the accused products. *See Anderson*, 477 U.S. at 248.

17 **A. SSLV and ProxySG cannot "communicate[] to" each other.**

18 In order to coordinate and successfully split the claimed SSL connection, claim 1 of the
 19 '580 patent requires the first and second security computers to be "communicatively coupled" and
 20 several limitations require the computers to "communicate[]" or "reply" to one-another. *See* '580
 21 patent at claim 1, 7:51-51, 7:62, 8:8-9, 8:17. Because, as explained above, SSLV is transparent, it
 22 is unable to be "communicate[d] to" or otherwise be "communicatively coupled" with ProxySG or
 23 any network device.

24 Because SSLV is transparent, it has no IP addresses and is not visible to other devices on
 25 the network; the other network devices are unaware of its presence. *See* Exh. 23 (BC2-1607593).
 26 Finjan does not dispute these facts. Exh. 21 (Cole Dep. Tr.) at 39:2-21. It is also undisputed that a
 27 device must at least be aware that another device exists on the network in order to communicate
 28 with it. *Id.* at 47:15-19 ("You would have to know that the device is on the network to

1 communicate with it.”). [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 Acknowledging this obvious discrepancy between the claim and the accused products,
 6 Finjan alleges instead that SSLV can “intercept” messages communicated between ProxySG and
 7 the client. *See* Exh. 21 (Cole Dep. Tr.) at 44:18-21. But even Finjan acknowledges that
 8 intercepted messages are “communicated to a different destination” than the interceptor. Exh. 22
 9 (Medvidovic Dep. Tr.) at 113:24-114:4. By way of analogy, while an undetected third party who
 10 has wiretapped a phone conversation may be able to “intercept” a conversation between a caller
 11 and recipient, neither party is communicating to (or replying to) the eavesdropper. This
 12 distinction is critical with respect to the ’580 patent because the claimed communications require
 13 an awareness and cooperative exchange between the two security gateways; to successfully “split”
 14 the SSL connection, these messages include content intended for use by the targeted recipient.
 15 *See, e.g.*, ’580 patent at 5:18-21 (“In order that the certificate cache at security gateway A be up-
 16 to-date, security gateway B sends updated server certificates to security gateway A when the
 17 server certificates change.”). Accordingly, SSLV’s undetected interception of communications
 18 from ProxySG to the client does not satisfy the “communicat[ion]” limitations of claim 1.

19 **B. ProxySG and SSLV cannot communicate a “reply message” or “cached**
 20 **attributes of the signed server certificate” to each other and do not have a**
 21 **“certificate comparator.”**

22 As explained above, the system claimed by the ’580 patent operates such that the second
 23 security computer checks and updates the cached certificate attributes sent by the first security
 24 computer. ’580 patent at 5:22-6:42. This is necessary in order to “split” the SSL connection
 25 between the two computers; while the first security computer is unable to communicate with the
 26 SSL content server, it maintains its own copy of the content server’s certificate for establishing a
 27 connection with the client. Claim 1 includes several limitations directed to this operation. In sum,
 28 claim 1 requires (a) the first security computer to send the attributes of its stored certificate to the
 second security computer along with a connection request, (b) the second security computer to

1 compare these stored attributes to the current certificate's attributes, and (c) the second security
 2 computer to reply with updated attributes, if necessary, for the first security computer to revise its
 3 cached certificate. None of these steps are performed by the accused Blue Coat products.

4 Specifically, claim 1 of the '580 patent requires that the first security computer send "a
 5 connection request message . . . including cached attributes of the signed certificate" to the second
 6 security computer. '580 patent at claim 1, 7:62-8:2. [REDACTED]

7 [REDACTED]
 8 [REDACTED]
 9 [REDACTED]
 10 [REDACTED]
 11 [REDACTED]
 12 [REDACTED]
 13 [REDACTED]
 14 [REDACTED]
 15 [REDACTED]
 16 [REDACTED]

17 Accordingly, there is no "connection request message including cached attributes of the signed
 18 certificate" communicated between the accused Blue Coat products.

19 Similarly, SSLV does not send any "cached attributes of the signed certificate" to ProxySG
 20 or to the content server, either as part of a connection request or as part of any subsequent
 21 communication. *See id.* Indeed, Dr. Cole does not include **any** opinion regarding this element,
 22 much less any evidence, in his report. *See* Exh. 3 (Cole Rpt.) at ¶¶ 1795-98. Again, this is simply
 23 not part of Blue Coat's architecture; SSLV does not need a "second security computer" to check
 24 whether certificate attributes are up-to-date and, therefore, does not send attributes anywhere.

25 Claim 1 further requires that the second security computer have "a certificate comparator
 26 _____

27 ⁴ As stated above, Finjan alleges that SSLV is the "first security computer" and ProxySG is the
 28 "second security computer." Exh. 21 (Cole Dep. Tr.) at 35:21-36:4. However, neither SSLV nor
 ProxySG is capable of performing the claim functions discussed herein.

1 for comparing the cached attributes of the signed certificate with the current attributes of the
2 signed certificate.” ’580 patent at claim 1, 8:12-14. [REDACTED]

3 [REDACTED]
4 [REDACTED] Thus, ProxySG does not receive anything that it can “compar[e] with the current attributes
5 of the signed certificate.” Unlike the system claimed by the ’580 patent, ProxySG does not
6 examine the certificates of other devices to determine if they are current; such a comparison does
7 not take place at all between the accused products. *See* Exh. 25 (BC2_SC_004547–627), ll. 3792-
8 3808, Exh. 26 (BC2_SC_004628–674), ll. 2589-2613.

9 Finally, claim 1 requires the second security computer to generate “a reply message” in
10 response to the connection request, which includes updated attributes of a server’s signed
11 certificate if the cached attributes “do not match the current attributes.” ’580 patent at claim 1. As
12 discussed, [REDACTED]

13 [REDACTED] Accordingly, it cannot and does not
14 send a “reply message communicated to said first security computer, when . . . the cached
15 attributes of the signed certificate do not match the current attributes of the signed certificate.” *Id.*
16 at claim 1, 8:16-20. Even Finjan acknowledges that no “reply message” is sent by the accused
17 Blue Coat products. *See* Exh. 21 (Cole Dep. Tr.) at 61:23-62:7 (“Q. [Y]ou don’t use the word
18 ‘reply’ anywhere in your opinion . . . ? A. No. But if you look at the descriptive language, it’s
19 implied in the use of the word ‘received.’”). Moreover, because SSLV is transparent, ProxySG
20 cannot send and SSLV cannot “receiv[e] . . . a reply message.” *See* Exh. 23 (BC2-1607593); Exh.
21 21 (Cole Dep. Tr.) at 47:15-19.

22 The limitations of claim 1 reflect a deliberate communication scheme between two security
23 computers that coordinate to “split” an SSL connection, which has certain technical requirements.
24 Because SSLV and ProxySG provide no such functionality, they cannot meet the limitations.

25 **C. SSLV and ProxySG do not share the claimed “non-SSL connection.”**

26 Claim 1 of the ’580 patent requires the first and second security computers be
27 “communicatively coupled . . . via a non-SSL connection.” ’580 patent at claim 1, 7:62-63. As
28 explained above, this limitation is at the very core of the ’580 patent’s invention: the ’580 patent

1 describes “splitting an SSL connection between gateways,” by creating a “non-SSL connection”
2 between them. *See id.* at 3:24-27. SSLV and ProxySG share no such connection.

3 Per the ’580 patent, the claimed “non-SSL connection” allows the second security
4 computer to decrypt SSL traffic received from the content server and send the unencrypted content
5 to the first security computer where the content is reencrypted in SSL and then transmitted to the
6 client. *See, e.g., id.* at Fig. 2; 4:1-5. Any number of intermediary computers between the two
7 security computers therefore have access to the content without needing to form SSL connections.
8 *See id.* at 1:66-2:2. This is what distinguishes the ’580 patent from the prior art. *See id.* at Figs.
9 1A-2; Exh. 22 (Medvidovic Dep. Tr.) at 329:11-24 (“[O]ne way that the communication is more
10 efficient is that—simply that the data itself is not encrypted.”).

11 SSLV and ProxySG do not operate this way. Instead, it is undisputed that SSLV and
12 ProxySG must each independently decrypt and reencrypt SSL traffic before it is returned to the
13 client or otherwise transmitted for additional inspection. *See* Exh. 7 (BC2-0024427) (“Use the
14 SSL Visibility Appliance with the ProxySG . . . In this architecture SSL traffic is decrypted twice,
15 once on the ProxySG and then again on the SSL Visibility Appliance”); [REDACTED]

16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED] [REDACTED]
27 [REDACTED]
28 [REDACTED]

1 [REDACTED]

2 Another byproduct of its ill-conceived infringement read, Finjan's only assertion as to the

3 existence of the required "non-SSL connection" is that the claimed connection exists for SSLV to

4 send a connection request message to ProxySG. *See* Exh. 21 (Cole Dep. Tr.) at 72:16-73:7. But

5 the alleged non-SSL connection Finjan points to can only exist prior to the establishment of *any*

6 SSL connection. *See id.* at 75:3-9 ("Q. The connection request message to which you refer

7 happens before the SSL session begins, correct? . . . A. Yes, before the session between the client

8 and the server."). In other words, every SSL connection *begins* with an unencrypted connection

9 request message. *Id.* at 16:11-19:15. For Finjan to allege that such a connection message

10 constitutes a "non-SSL connection" would render the term "non-SSL" meaningless; every

11 connection is non-SSL before an SSL session is established, and claim 1 of the '580 patent has

12 nothing to do with such pre-SSL session connections. As Finjan's own expert witness admitted, a

13 non-SSL connection existing only *prior to* the SSL connection itself being established is

14 insufficient; the non-SSL connection must be maintained through the transaction. *See* Exh. 22

15 (Medvidovic Dep. Tr.) at 327:16-22 ("Q. So, between the [security computers], even though there

16 is an existing SSL connection on either side, the connection between the two is non-SSL? A.

17 Correct. And that's what—again that's what Figure 2 also talks about. Q. And that's in claim 1;

18 right? A. That's what claim 1 says."). Finjan's tortured infringement read eviscerates the claim

19 language, the purported advantage of the patent, and the only sensible interpretation of the claim.

20 **D. SSLV does not perform an "SSL handshake with the client computer."**

21 Claim 1 requires the first security computer to perform an "SSL handshake with the client

22 computer." '580 patent at claim 1, 7:59-60; *see also* Exh. 21 (Cole Dep. Tr.) at 63:14-23 (stating

23 claim 1 requires all steps of SSL handshake). SSLV does not perform such a handshake.

24 As discussed, SSLV is a transparent device and is not visible on the network. *See* Exh. 23

25 (BC2-1607593). [REDACTED]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED] The accused Blue Coat products therefore do not satisfy the limitation requiring the
7 first security computer perform an “SSL handshake with the client computer.” Accordingly, Blue
8 Coat does not infringe claim 1 of the ’580 patent. *See Litton Sys. Inc.*, 140 F.3d at 1454.

9 **V. Blue Coat Does Not Infringe Claim 22 of the ’408 Patent (“The Parse Tree Patent”).**

10 The ’408 patent is directed to “[a] method for scanning content, including identifying
11 tokens within an incoming byte stream, the tokens being lexical constructs for a specific language,
12 identifying patterns of tokens, generating a parse tree from the identified patterns of tokens, and
13 identifying the presence of potential exploits within the parse tree.” ’408 patent at Abstract, 2:26-
14 31. The claimed exploits are portions of malicious program code. *Id.* at claim 22, 21:55-57. To
15 that end, the ’408 patent describes “three main components: a tokenizer . . . a parser . . . and an
16 analyzer” to carry out the performance of the claimed invention. *See id.* at 2:35-46. While relying
17 on a “generic architecture,” the ’408 patent envisions a system that can be easily “customized for a
18 specific language through use of a set of language-specific rules.” *Id.* at 6:17-20. As such, the
19 selection of the correct “set of rules for the specific language” is central to the successful
20 identification of tokens, patterns, and ultimately potentially malicious program code. *See id.* at
21 Abstract, 2:31-34, 2:43-46. Another key feature claimed by the ’408 patent is its ability to
22 dynamically analyze a content stream while it is incoming (*i.e.*, in real-time). *See, e.g., id.* at 2:20-
23 24 (“Thus it may be appreciated that the present invention is able to diagnose incoming content.
24 As such, the present invention achieves very accurate blocking of content, with minimal over-
25 blocking as compared with prior art scanning technologies.”); *see also id.* at 5:55-58 (“ARB 55
26 scanner 130 performs much more intensive processing than pre-scanner 150, and processes
27 incoming content at a rate of approximately 1 mega-bit per second.”). As the ’408 patent explains,
28

1 the advantage of dynamic analysis is the ability to act upon malicious content in real-time,
 2 increasing the accuracy with which content is blocked. *See id.*

3 In accusing Blue Coat's WebPulse product—and, in particular, the DRTR component of
 4 WebPulse—of infringing claim 22 of the '408 patent,⁵ Finjan takes the incredible position that file
 5 types constitute “programming languages.” DRTR is simply not designed to perform the code
 6 parsing techniques contemplated by the '408 patent. [REDACTED]

7 [REDACTED]
 8 [REDACTED]
 9 [REDACTED]
 10 [REDACTED]
 11 [REDACTED]
 12 Moreover, DRTR does not analyze content while it is incoming, but rather only after it is
 13 downloaded completely. *See* Exh. 27 (BC2_SC_000001-055), ll. 570-583. Thus, Finjan's
 14 technically untenable arguments aside, the Blue Coat products that Finjan accuses do not infringe
 15 claim 22 of the '408 patent such that Blue Coat is entitled to judgment as a matter of law. *See*
 16 Fed. R. Civ. P. 56; *Anderson*, 477 U.S. at 248.

17 **A. DRTR does not “determin[e] any specific one of a plurality of programming**
 18 **languages.”**

19 Claim 22 of the '408 patent requires “determining any specific one of a plurality of
 20 programming languages in which the incoming stream is written.” '408 patent at claim 22, 21:46-
 21 47. The claim requires that such a determination must be made from among a set of more than
 22 one programming language. None of the accused Blue Coat products make such a determination.
 23 Specifically, DRTR does not perform the required determination of a specific programming
 24 language from among a plurality of programming languages.⁶

25 _____
 26 ⁵ Finjan also accuses WSS via its alleged use of WebPulse. Exh. 2 (Mitzenmacher Rpt.) at ¶ 21.

27 ⁶ While Finjan accuses multiple Blue Coat products of infringing the '408 patent, it is clear the
 28 accused functionally across all products lies within DRTR. [REDACTED]
 [REDACTED]

1 When processing a downloaded file, DRTR can determine certain file characteristics
2 relevant to content categorization, none of which are programming languages. [REDACTED]

3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED] These file types are not programming languages because each file type can consist of a
10 variety of languages, or no programming language at all. As acknowledged by Finjan's expert, it
11 is undisputed that identifying a file as "executable" accomplishes only that; it does not identify the
12 specific programming language in which the file is written. *See id.*; [REDACTED]

13 [REDACTED]
14 Finjan also takes the position that DRTR can determine a programming language by
15 detecting whether a URL contains HTML. *See* Exh. 2 (Mitzenmacher Rpt.) at ¶ 923. This is
16 simply false. [REDACTED]

17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 Furthermore, after the initial file type determination, [REDACTED]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED] Put simply, at most, the presence of
9 these tags is merely an indication that one of any number of programming languages may exist
10 within. *See* Exh. 11 (C. Larsen Dep. Tr.) at 237:19-238:1. Accordingly, [REDACTED]
11 [REDACTED] DRTR need not and does not “determin[e] any specific one of
12 a plurality of programming languages in which the incoming stream is written.”

13 **B. DRTR does not “instantiate[e] a scanner . . . in response.”**

14 Because DRTR does not “determin[e] any specific one of a plurality of programming
15 languages” as explained above, it also cannot and does not “instantiate[e] a scanner for the specific
16 programming language, in response to said determining.” At most, [REDACTED]
17 [REDACTED]

18 **C. DRTR does not analyze an “incoming stream” of program code.**

19 As explained above, the system claimed by the ’408 patent operates on “an incoming
20 stream of program code.” ’408 patent at claim 22, 21:45. Claim 22 includes several limitations
21 directed to this aspect of operation. Claim 22 first requires “receiving an incoming stream of
22 program code,” “determining any specific one of a plurality of programming languages in which
23 the incoming stream is written,” and then “identifying individual tokens within the incoming
24 stream.” *See id.* at claim 22, 21:45-58. Claim 22 also requires “dynamically building, while said
25 receiving receives the incoming stream” and “indicating the presence of potential exploits within
26 the incoming stream.” *See id.* at claim 22, 21:59-67. But none of the accused Blue Coat products
27 operate in such a manner. [REDACTED]
28 [REDACTED]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 Finjan's expert provides *no* particular analysis for this claim element in his report. Indeed,
9 Dr. Mitzenmacher instead admits [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED] But claim 22 is explicit, and
14 requires "dynamic[] building, *while* said receiving receives the incoming stream." The undisputed
15 operation of DRTR simply does not satisfy that requirement.

16 Thus, the accused Blue Coat products neither determine a specific one of a plurality of
17 programming languages in which the steam is written, nor perform analysis of content on "an
18 incoming stream." Accordingly, Blue Coat does not infringe claim 22 of the '408 patent. *See*
19 *Litton Sys. Inc.*, 140 F.3d at 1454.

20 **VI. Blue Coat Does Not Infringe Claim 1 of the '786 Patent.**

21 In its infringement allegations as to the '786 patent, Finjan again accuses products that
22 reflect a fundamentally different network security architecture than what is described by the
23 asserted patent. The '786 patent is generally directed to detecting untrusted code in a
24 Downloadable and transmitting mobile protection code with the Downloadable to a destination
25 device for execution. *See* '786 patent at Abstract. The Court has found that "mobile protection
26 code" means "code that, at runtime, monitors or intercepts actually or potentially malicious code
27 operations." *See Finjan Inc. v. Blue Coat Sys., Inc.*, No. 13-03999 BLF, 2014 WL 5361976 (N.D.
28 Cal. Oct. 20, 2014). The specification explains the formation of the package including mobile

1 protection code, i.e. the sandbox: “a protection engine retrieves protection parameters and forms
 2 mobile protection code according to the parameters. The protection engine further, in step 1013,
 3 retrieves protection parameters and forms protection policies according to the parameters. Finally,
 4 in step 1015, the protection engine couples the mobile protection code, protection policies and
 5 received-information to form a sandboxed package.” *See* ’786 patent at 20:27-36.

6 Crucially, the method of claim 1 further requires that the “the sandboxed package . . . be
 7 communicated to the . . . information-destination.” *See id.* at claim 1, 21:47-48. The specification
 8 explains that the “information-destination” is the requesting client’s user device, and no other
 9 exemplary destinations—no intermediary computers or other inspection devices—are recited in
 10 the patent. *See, e.g., id.* at Figs 1b, 1c, 7:14 (referring to “user devices or ‘Downloadable-
 11 destinations’” interchangeably); 8:35-39 (referring to “information-destination or ‘user device’”
 12 interchangeably); 11:65-12:3 (referring to the destination as the “client”). The “destination” is the
 13 machine that the claimed system seeks to protect. *See, e.g., id.* at 10:3-49. This, of course, makes
 14 sense in light of the disclosed invention—mobile protection code makes Downloadables safer to
 15 operate in an exposed environment, such as a client; it is not necessary for execution of a
 16 Downloadable on a purpose-built security device.

17 The Blue Coat products that Finjan accuses take a diametrically different approach to
 18 sandboxing.⁷ While the system of the ’786 patent envisions a protection scheme in which
 19 suspicious files are packaged safely and then executed on the requesting client machine, the
 20 accused Blue Coat products offer a system in which suspicious files are executed at the gateway in
 21 a safe environment before being sent to the requesting client machine. *See* Exh. 32 (Harrison Dep.
 22 Tr.) at 124:13-17 (“Malware Analysis appliance is designed to receive the image of a file,
 23 typically a binary, and it causes that program or file to execute in a controlled environment where
 24 it can assess its behavior—record and assess its behavior, and then make a determination as to
 25 whether or not that behavior appears to be suspicious or malicious in some way.”). Only MAA

26
 27 ⁷ While Finjan accuses a host of products in the Blue Coat ecosystem—WebPulse/GIN, WSS with
 28 MAS, ASG with MAA, ProxySG and CAS with MAA—of infringing claim 1 of the ’786 patent,
 the necessary and primary accused functionality resides in MAA. *See* Exh. 3 (Cole Rpt.) at ¶ 26.

1 performs sandboxing. *See id.* In fact, MAA is a dedicated sandboxing and inspection device; its
 2 entire purpose is to check files before they are ever transmitted to clients. *See id.* Thus, allowing
 3 execution to take place on the accused intermediary appliance, rather than on the requesting client
 4 machine, is at the heart of the Blue Coat system. This critical difference results in a number of
 5 elements of claim 1 of the '786 patent being absent from the accused Blue Coat products. Despite
 6 advancing its strained infringement theories, Finjan cannot dispute the actual functionality of
 7 MAA. Thus, there remains no genuine issue of material fact such that a reasonable jury could
 8 return a finding of infringement. *See Anderson*, 477 U.S. at 248.

9 **A. No “sandboxed package including the mobile protection code . . . [is]**
 10 **communicated.”**

11 Claim 1 of the '786 patent includes a number of limitations, among them “causing . . .
 12 mobile protection code to be communicated,” claimed as comprising “forming a sandboxed
 13 package including the mobile protection code and the downloadable-information. . . to be
 14 communicated.” '786 patent at claim 1, 21:39-48. MAA neither sends nor receives the claimed
 15 “sandboxed package including the mobile protection code.”

16 As explained above, MAA is a dedicated appliance whose sole purpose is to scan and run
 17 unknown files before they are transmitted to clients. *See* Exh. 33 (Birkeland Dep. Tr.) at 11:16-
 18 25. To this end, MAA performs dynamic analysis on a received executable. *See* Exh. 34 (Rohan
 19 Dep. Tr.) at 117:13-118:3. For dynamic analysis, rather than reading the code of the file to check
 20 for signatures, the file is actually run, and the operations it performs are monitored. *See* Exh. 33
 21 (Birkeland Dep. Tr.) at 11:16-25. [REDACTED]

22 [REDACTED]
 23 [REDACTED]
 24 [REDACTED]
 25 [REDACTED]
 26 [REDACTED] Thus, in light of MAA’s singular responsibility for
 27 sandboxing executables, the appliance need not and does not perform the requisite communication
 28 of the “mobile protection code” or the “sandboxed package including the mobile protection code.”

1 Unable to formulate a coherent theory of infringement by MAA, Finjan tries to allege that
 2 “parameters” and “information” transmitted to MAA along with the executable file constitute the
 3 claimed “mobile protection code.” But Finjan does not and cannot explain how “parameters” can
 4 be “code” that “monitors or intercepts operations.” *See, e.g.*, Exh. 22 (Medvidovic Dep. Tr.) at
 5 70:20-22, 75:12-16 (“Code is some sort of representation of a computer program. . . . [Y]ou can’t
 6 just write, ‘I’d like to have a method here called Fu and it’s going to have these parameters’ . . . it
 7 has to respect the syntax of language.”). Finjan’s expert recognized the difference between
 8 parameters providing configuration information and providing the actual code. [REDACTED]

9 [REDACTED]
 10 [REDACTED]. The ’786 patent also
 11 recognizes the distinction, explaining that the claimed “protection engine retrieves protection
 12 parameters and forms mobile protection code *according to* the parameters.” ’786 patent at 20:27-
 13 31 (emphasis added). Accordingly, protection parameters can inform the production of mobile
 14 protection code, but cannot comprise the code itself and therefore fail to satisfy the limitations of
 15 claim 1 requiring communication of mobile protection code.

16 **B. MAA is not an “information-destination.”**

17 As explained above, the invention claimed by the ’786 patent requires that the sandboxed
 18 package be transmitted to the requesting client’s user device. *See* ’786 patent at 8:35-39. Claim 1
 19 therefore includes multiple limitations directed to this requirement, none of which are performed
 20 by the accused Blue Coat products. Specifically, the accused products not do not “caus[e] . . .
 21 mobile protection code to be communicated to at least one information-destination” or “caus[e]
 22 the sandboxed package to be communicated to the at least one information-destination.”

23 As explained, in the accused Blue Coat system, sandboxing is performed entirely on the
 24 MAA network appliance, rather than on the client system. *See* Exh. 33 (Birkeland Dep. Tr.) at
 25 11:16-25. The only infringement theory available to Finjan is to insist that MAA constitutes the
 26 “information-destination.” However, the ’786 patent requires that the claimed “information-
 27 destination” is the client user device that requested the “downloadable-information.” *See, e.g.*,
 28 ’786 patent at 7:14; 8:35-39; 11:65-12:3. The specification uses “information-destination” and

1 “user device” interchangeably. *See id.* The specification also makes clear that the information-
 2 destination is the “protected” machine within the claimed system. *See, e.g., id.* at 19:31-46.
 3 Accordingly, MAA cannot be the claimed “information-destination” because it is neither the
 4 requesting user device nor the object of protection in the accused system. Because MAA is not the
 5 claimed “destination,” the accused products fail to satisfy the requirement that “mobile protection
 6 code” within “the sandboxed package be communicated to the . . . information-destination.”

7 **C. Blue Coat products do not infringe the ’786 patent under the doctrine of**
 8 **equivalents.**

9 Of the asserted patents addressed in this motion, Finjan alleges that the accused Blue Coat
 10 products infringe only the ’786 patent under the doctrine of equivalents. *See* Exh. 3 (Cole Rpt.) at
 11 ¶ 27. But equivalence must be proven by “showing on a limitation-by-limitation basis that the
 12 accused product performs substantially the same function in substantially the same way with
 13 substantially the same result as each claim limitation of the patent[]” *Wavetronix LLC v. EIS*
 14 *Electronic Integrated Systems*, 573 F.3d 1343, 1360 (Fed. Cir. 2009). Moreover, the doctrine of
 15 equivalents cannot be used to vitiate an element of the claim. *Asyst Technologies, Inc. v. Emtrak,*
 16 *Inc.*, 402 F.3d 1188, 1195 (Fed. Cir. 2005) (“To hold that ‘unmounted’ is equivalent to ‘mounted’
 17 would effectively read the ‘mounted on’ limitation out of the patent.”). Here, the accused Blue
 18 Coat products do not provide the same function, in the same way, and with the same result as the
 19 limitations of claim 1 requiring “packaging engine mobile protection code to be communicated to
 20 at least one information-destination of the downloadable-information . . . wherein the causing
 21 mobile protection code to be communicated comprises forming the packaging engine a sandboxed
 22 package including the mobile protection code and the downloadable-information, and causing the
 23 sandboxed package to be communicated to the at least one information-destination.”

24 The function of these limitations is to provide the information-destination of the
 25 downloadable (*e.g.*, the requesting “user device”) with a sandbox package based on that
 26 information-destination’s security policies. *See* ’786 patent at 10:56-11:43. The sandboxed
 27 package can be run in place of the downloadable, with policy-specific operations protected by the
 28 mobile protection code. *Id.* Thus, the mobile protection code is designed to protect the user

1 device while running the downloadable, such that violations of the security policies are blocked in
 2 real time. *Id.* at 20:44-21:16. In sharp contrast, the function of MAA is to “detonate” a sample in
 3 a purpose-built environment to determine its behaviors and risk level so that information-
 4 destinations (*e.g.*, the requesting “user devices”) can be protected from ever receiving a dangerous
 5 file. *See supra* 19-20. In other words, the function of claim 1 of the ’786 patent is to prevent the
 6 performance of malicious attacks by files already received at the destination computer, while the
 7 function of the Blue Coat products is to observe the performance of malicious attacks to gather
 8 data about unknown files that could be dangerous before sending the files to the destination.

9 Consequently, the way in which these two functions are achieved is distinctly different.
 10 Whereas the claimed invention of the ’786 patent intercepts a downloadable and packages it with
 11 protection code based on an information-destination’s profile before sending it to that destination
 12 for execution, MAA receives a downloadable and performs analysis locally, using code resident
 13 on MAA itself. [REDACTED]

14 [REDACTED]
 15 [REDACTED]
 16 Finally, the results achieved by the limitations of claim 1 of the ’786 patent are not the
 17 same as those achieved by the accused Blue Coat products. The ’786 allows a requesting
 18 information-destination to run a downloadable in a relatively safe manner while decreasing the
 19 load on network infrastructure, making no advance attempt to determine if the downloadable is
 20 suspicious because it hopes to block such operations in real time. The file is always delivered to
 21 the destination regardless of risk. In contrast, MAA allows suspicious operations to occur to
 22 determine if they pose a threat and, based on that determination, can prevent the file from ever
 23 being delivered. Put another way, MAA does nothing to protect an end user device; it simply
 24 prevents the file from being delivered to that device in the first place if it identifies a risk.

25 The above claim limitations are not satisfied by the accused Blue Coat products under the
 26 doctrine of equivalents. *See Wavetronix LLC*, 573 F.3d at 1360. As discussed above, claim 1 of
 27 the ’786 patent is also not directly infringed. *See Litton Sys. Inc.*, 140 F.3d at 1454.

28 **VII. Blue Coat’s “WebPulse/GIN” Product Does Not Perform Sandboxing.**

1 In its attempt to implicate as many Blue Coat products and services as possible, Finjan's
2 allegations as to the '844, '494, '786, '621, and '086 patents include accusations of infringement
3 by "WebPulse/GIN sandboxing." [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

1 [REDACTED]
 2 [REDACTED]
 3 [REDACTED]
 4 [REDACTED]
 5 [REDACTED]
 6 [REDACTED]
 7 [REDACTED]
 8 [REDACTED]
 9 [REDACTED]
 10 [REDACTED]
 11 [REDACTED]
 12 [REDACTED]
 13 [REDACTED]

14 [REDACTED] *See* 35 U.S.C. § 271(a); *see also*
 15 *Rotec Indus., Inc. v. Mitsubishi Corp.*, 215 F.3d 1246, 1251 (Fed.Cir.2000) (“[E]xtraterritorial
 16 activities . . . are irrelevant to the case before us, because the right conferred by a patent under our
 17 law is confined to the United States and its territories, and infringement of this right cannot be
 18 predicated on acts wholly done in a foreign country.”) (internal citations omitted).

19 [REDACTED]
 20 [REDACTED] Even if Finjan’s allegations were
 21 correct, they do not support a finding of infringement as to “WebPulse/GIN” sandboxing where
 22 the only allegedly infringing activity takes place entirely on MAA. The alleged integration of
 23 “WebPulse/GIN” is unrelated to any element of the asserted claims—even by Finjan’s own
 24 account—and Finjan’s transparent attempt to ensnare additional products should be rejected.

25 **VIII. CONCLUSION**

26 For the foregoing reasons, Blue Coat respectfully requests that the Court grant summary
 27 judgment of noninfringement for all asserted claims of the ’580, ’408, and ’786 patents and as to
 28 all sandboxing allegations against WebPulse/GIN.

1 Dated: May 17, 2017

Respectfully submitted,

2 WILSON SONSINI GOODRICH & ROSATI
3 Professional Corporation

4
5 By: /s/ Stefani E. Shanberg
Stefani E. Shanberg

6 Attorneys for Defendant
7 BLUE COAT SYSTEMS LLC
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28